



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Se

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,378	11/16/2001	Dorothy E. Denning	774070-8	7029
23879	7590	04/07/2005	EXAMINER	
BRIAN M BERLINER, ESQ O'MELVENY & MYERS, LLP 400 SOUTH HOPE STREET LOS ANGELES, CA 90071-2899			POLTORAK, PIOTR	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/992,378	Applicant(s) DENNING ET AL.	
	Examiner Peter Poltorak	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 November 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-50 have been examined.

Priority

2. Acknowledgment is made of applicant's claim for priority based on a continuation-in-part of co-pending patent application: 09/699832 filed on October 30, 2000 and 09/758637 filed on January 10, 2001.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-27 and 36 are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention.
4. In claim 1 it is not clear whether an "encrypted data encrypting key" lacks antecedent basis or whether the term refers to a "data encrypting key".
5. The term "universal location" in claim 5 is not understood. The term is directed towards the location and it is used to represent "the entire earth". However, claim 1 defines a location identity attribute that defines at least a specific geographic location and claim 2 further limits the location identity comprising at least a location value and a proximity value. Also, the specification defines location value as corresponding to the unique

geographic position of a particular place. It is not clear how a pint-point location can encompass the entire earth.

6. The term "corresponds to a zone" in claim 6 is not understood.
 7. The term "a shape parameter" in claims 10, 12 and 36 is not understood
 8. The term "rendering unusable said encrypted digital information" in claims 14-15 and 46" is not understood.
 9. Claims 2-3, 7-9, 11, 13 and 16-27 are rejected by virtue of their dependence.
- Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1-4, 6-16, 28-31, 32-39, 45-47 are rejected under 35 U.S.C. 103(a) as

being unpatentable over *Menezes (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237)* in view of *Murphy (U.S. Patent No. 6317500)*.

11. As per claims 1 and 13 (as best understood) *Menezes* teaches encrypting digital information using a data encrypting key which generates the encrypted digital information (*Menezes, pg. 16 Fig. 1.7*), which also reads on associating the encrypted data encrypting key with the encrypted digital information that could be accessed only at a specific location, and encrypting the data

encrypting key using a key encrypting key (*Menezes, "Point-to-point key update using symmetric encryption", in particular "key transport with one pass" section, pg. 497-498*).

12. *Menezes* does not explicitly teach using information derived from a location identity attribute that defines at least a specific geographic location in the encryption process.
13. *Murphy* discloses a module containing an encryption chip that includes a Global Positioning System (GPS) in order to obtain the location coordinates of a receiver (*the licensed site*), wherein the coordinates are used to enforce that only the receiver at the location can decrypted send digital content (*Murphy, col. 7 line 55 - col. 8 line 28 and col. 6 lines 46-65*), which reads using information derived from a location identity attribute that defines at least a specific geographic location in the encryption process.
14. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use information derived from a location identity attribute that defines at least a specific geographic location in the encryption process as taught by *Murphy*. One of ordinary skill in the art would have been motivated to perform such a modification in order to control distribution of digital content authorized for specified locations or sites (*Murphy, col. 7 lines 6-10*).
15. As per claims 2-3 and 7-9 *Murphy* teaches the location identity attribute comprising at least a location value (*location coordinates $x(i)$, $y(i)$, $z(i)$*), and a proximity value (*the diameter $d(i)$ of the region $R(L(i), d(i))$*) of the specific

geographic location, the location value corresponding to a location of an intended receiver of the digital information, communicating the encrypted digital information to a receiver of the digital information disposed at the specific geographic location, and a location identifying step comprising recovering the location from a GPS receiver (*Murphy*, col. 7 line 55 - col. 8 line 28 and col. 6 lines 46-65).

16. As per claim 4 GPS location inherently describes the longitude and latitude of a location.

17. As per claim 6 (as best understood) the proximity value inherently corresponds to a zone that encompasses the location.

18. As per claim 10 (as best understood) a proximity value reads on a shape parameter.

19. As per claims 11 and 12 *Menezes*' teaching discussed above includes decrypting the data encryption key using the key decrypting key and decrypting the digital information using the data encryption key, and *Murphy*'s teaching involves a sender and a receiver using location values from a signal received by a GPS.

20. The limitations of claims 14 and 15 (as best understood) are implicit. Without the decrypted key encrypted digital information is unusable and *Murphy* teaches that the decryption process cannot be performed at other than the specific geographic location (*Murphy*, col. 6 lines 46-65).

21. Claim 16 is implicit. Placing limitations of using session keys and/or preventing decryption at other than a designated location would not make

sense if two entities were directly connected without any intermediate nodes (*distributors*) e.g. routers in between them.

22. Claims 28-31, 32-38 and 45-47 are substantially equivalent to claims 1-4, 6-11 and 14; therefore claims 28-31, 32-38 and 45-47 are similarly rejected.

23. Claims 18-19 and 39 are rejected under 35 U.S.C. 103(a) as being anticipated unpatentable over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Murphy* (U.S. Patent No. 6317500) and in further view of *Schneier* (*Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457*).

24. *Menezes* and *Murphy* teach the data encryption key as discussed above.

As per claim 18 *Menezes* and *Murphy* do not explicitly teach generating the data encryption key using a pseudo-random number generator.

Schneier teach generating the data encryption key using pseudo-random number generator (*Schneier, pg. 173, Random Keys section*). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to generate the data encryption key using pseudo-random number generator as taught by *Schneier*. One of ordinary skill in the art would have been motivated to perform such a modification in order to assure appropriate strength of the key (*Schneier, pg. 170-173*).

As per claim 19, *Menezes* and *Murphy* do not explicitly teach that generating the encryption key comprises using GPS signals to partially seed the pseudo-random number generator. However, the choice of utilizing GPS signals

would have been obvious to one of ordinary skill in the art at the time of applicant's invention to provide the range of signals and constant changes in satellite positioning. One of ordinary skill in the art would have been motivated to utilize GPS signals to partially seed the pseudo-random number generator in order to take advantage of the large set of possible and constantly changing data that decrease predictability of the choice.

Claim 39 is substantially equivalent to claim 18; therefore claim 39 is similarly rejected.

25. Claims 5, 21-27 and 41-44 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Murphy* (*U.S. Patent No. 6317500*) and *Schneier* (*Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457*) and in further view of *Shibata et al.* (*U.S. Patent No. 5586185*).

26. As per claim 5 (as best understood) *Menezes* in view of *Murphy* teach location value as discussed above. The location value is to enforce using encryption only in a specific location (*Murphy, col. 8 lines 6-24*). However, it is well known in the art that certain signals may not be intended for just the specific location (e.g. broadcast) and also that some situations may need portability (e.g. travel with a laptop). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a universal location that encompasses the entire earth within the location value.

One of ordinary skill in the art would have been motivated to perform such a modification in order to provide security whenever there is a need to lift the limit on the location at which the data can be received.

27. As per claim 21 *Menezes* and *Murphy* teach storing the key encrypting key.

Menezes and *Murphy* do not explicitly teach a key table used for storing a plurality of keys including a key encrypting key.

Shibata et al. teach a key table for storing a plurality of keys (*Shibata et al.*, col. 1 line 55 – col. 2 line 23).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a table to store a plurality of keys (including a key encrypting key) as taught by *Shibata et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to allow secure communication for multiple providers (*Shibata et al.*, col. 1 lines 7-67).

As per claims 22-25 *Shibata et al.* teach associating the plurality of keys with respective providers of the digital information, remote administering management comprising adding, changing or deleting any one of the plurality of keys in the key table (*Shibata et al.*, col. 1 line 55 – col. 2 line 23).

28. As per claim 26 and 27 *Menezes* teaches keys for signing data and validating signatures (*Menezes*, pg. 28). Furthermore, *Menezes* teaches that digital signature provides authentication, authorization, and non-repudiation.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include keys for signing data, to validate signatures and include a signature when adding, changing or deleting any one of the

Art Unit: 2134

plurality of the secret keys in the key table. One of ordinary skill in the art would have been motivated to perform such a modification in order to establish authenticity of the keys (*authentication and non-repudiation*).

29. Claims 41-44 are substantially equivalent to claims 21-22, 24 and 26;

therefore claims 41-44 are similarly rejected.

30. Claims 1, 11, 16-17, 20, 28, 37-38, 40, 45 and 48 are rejected under 35

U.S.C. 103(a) as being unpatentable over *Inoue et al.* (U.S. Patent No. 6240514) in view of *Murphy* (U.S. Patent No. 6317500).

31. As per claims 1 and 20 (as best understood) *Inoue et al.* teaches encrypting digital information using a data encrypting key which generates the encrypted digital information, which reads on associating the encrypted data encrypting key with the encrypted digital information that could be accessed only at a specific location, encrypting the data encrypting key using a key encrypting key, decrypting the encrypted data encrypting key, and re-encrypting the data encrypting key using a different encrypting key (*Inoue et al.*, col. 4 line 49- col. 5 line 3).

32. As per claim 11 *Inoue et al.* teach decrypting and re-encrypting packets (*Abstract*).

33. *Inoue et al.* does not explicitly teach using information derived from a location identity attribute that defines at least a specific geographic location in the encryption and decryption process.

34. *Murphy* discloses a module containing an encryption chip that includes a Global Positioning System (GPS) in order to obtain the location coordinates of

a receiver (*the licensed site*), wherein the coordinates are used to enforce that only the receiver at the location can be decrypted and send digital content (*Murphy, col. 7 line 55 - col. 8 line 28 and col. 6 lines 46-65*), which reads using information derived from a location identity attribute that defines at least a specific geographic location in the encryption process.

35. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use information derived from a location identity attribute that defines at least a specific geographic location in the encryption process as taught by *Murphy*. One of ordinary skill in the art would have been motivated to perform such a modification in order to control distribution of digital content authorized for specified locations or sites (*Murphy, col. 7 lines 6-10*). Using at least one of a different location identity attribute would be implicit in re-encrypting the data encrypting key since the next node would be in a different location.

36. Claims 28, 40, 45 and 48 are substantially equivalent to claims 1, 11 and 20; therefore claims 28, 40, 45 and 48 are similarly rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Signature

3/18/05
Date


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100